The Health Foundation
Inspiring Improvement

Governance and HSCIC's IG Toolkit

Safe Settings

18-19 September 2015

The Health Foundation
Inspiring Improvement

In-house Governance

Technical solution

- Dedicated network
- Thin clients
- 256-bit Enhanced Encryption standard
- Firewalls
- Strict access controls
- 2 Factor authentication

It’s more than just tech!

- Good governance is required to underpin a Safe Setting
  - Who has admin rights on the system?
  - Who has the keys to the server room?
  - Who is authorised to release data or outputs?

- In fact, all ‘5 safes’ require good governance

- Both ISO 27001 and HSCIC IG Toolkit accreditation focus strongly on Governance

Governance at THF

Information Security Management Group (ISMG)

- COO
- Director of Data Analytics
- Head of Operations
- Head of IT
- IT Systems Manager
- Data Manager / Information Security Manager
- Senior Economic Fellow
- Economics Analyst
- Data Analyst

Governance at THF (2)

- Director's team approves IG policies
- ISMG approves IG procedures

- ISMG responsible for implementing, evaluating and improving policies and procedures

- We actively manage an Improvement Plan

- All policies and procedures are available in case of interest
  - (except Improvement Plan)

How do the 5 Safes fit in?

- Show Flow Chart

HSCIC's IG Toolkit

Background

- Submit an System Level Security Policy
- Reviewed by HSCIC's Technical Consultants
- Sign-off by IAO
- Interesting requests
  - DIM-level 5 Shredder

A flavour

Req No	Description	Action
Information Governance Management		
13-120	Responsibility for Information Governance has been assigned to an appropriate member, or members, of staff	View
13-121	There is an information governance policy that addresses the overall requirements of information governance	View
13-122	All contracts (staff, contractor and third party) contain clauses that clearly identify information governance responsibilities.	View
13-123	All staff members are provided with appropriate training on information governance requirements.	View
Confidentiality and Data Protection Assurance		
13-220	Personal information is only used in ways that do not directly contribute to the delivery of care services where there is a lawful basis to do so and objections to the disclosure of confidential personal information are appropriately respected	View
13-221	There are appropriate confidentiality audit procedures to monitor access to confidential personal information	View
13-222	All person identifiable data processed outside of the UK complies with the Data Protection Act 1998 and Department of Health guidelines	View
13-223	All transfers of personal and sensitive information are conducted in a secure and confidential manner	View
Information Security Assurance		
13-330	Policy and procedures ensure that mobile computing and teleworking are secure	View
13-331	There is an information asset register that includes all key information, software, hardware and services	View
13-332	Unauthorised access to the premises, equipment, records and other assets is prevented	View
13-333	There are documented incident management and reporting procedures	View
13-334	The confidentiality of service user information is protected through use of pseudonymisation and anonymisation techniques where appropriate	View
13-335	There are adequate safeguards in place to ensure that all patient/client information is collected and used within a secure data processing environment (safe haven) distinct from other areas of organisational activity.	View

A flavour (2)

0: Insufficient evidence to attain Level 1.

1: Responsibility for Information Governance has been assigned and an IG improvement plan has been developed.

The following criteria must **all** be satisfied:

a: Responsibility has been assigned for Information Governance

Evidence (recommended but not mandatory):

- Named individual(s) job description, or signed note or email assigning responsibility.

b: The named Information Governance staff have been provided with sufficient training to carry out their role.

c: The is an IG improvement plan that documents both the current level of compliance with the NHS IG requirements and the targets identified to progress to the next level of compliance.

2: The IG improvement plan has been approved by a senior staff member and is being implemented.

3: In-year reports and briefings on progress against the improvement plan are provided to senior management. IG arrangements are reviewed by a senior member of staff.

A flavour (3)

2: The IG improvement plan has been approved by a senior staff member and is being implemented.

The following criteria must **all** be satisfied:

a: The IG improvement plan has been signed off by a senior staff member.

Evidence (recommended but not mandatory):

- Sign off should be documented on the IG improvement plan, for example the date that it was signed-off and by whom.

b: The IG improvement plan has been implemented and gaps or weaknesses in current IG arrangements are being addressed.

Evidence (recommended but not mandatory):

- New guidance for staff or new organisational procedures of new ways or working.

Document everything

- Documents on
  - Responsibilities
  - Audits and spot-checks
  - Decision making processes
  - ISMG Minutes
  - Audit logs

Conclusion

- A Safe Setting encompasses more than just the techy bits!
- Decide as an organisation who is responsible for IG
  - No right or wrong way of doing it
- Getting accredited is an intensive process!
- Document what you do!

Keep in touch

For all the latest news and developments from the Health Foundation:

- Visit our website at **www.health.org.uk**
- Subscribe to our monthly email newsletter at **www.health.org.uk/newsletter**
- Register for email alerts to be notified about our latest work at **www.health.org.uk/updates**
- Take part in conversation and debate about current healthcare issues on our blog
- Follow us on Twitter, Facebook or LinkedIn.